

IV. REMARKS

The Examiner is thanked for extending the courtesy of a telephone interview on June 12, 2007. During this interview it was agreed that the rejection of claims 1 and 2 under 35 U.S.C. 102 on Adams also applies to claims 3 and 4.

The specification has been amended as requested except that the requested correction to page 6 has been done to page 3, which is where the designated error occurs. Thus the disclosure is no longer objectionable.

The claims have been amended as requested. Thus they are no longer objectionable.

Claims 1-4 are not unpatentable under 35 U.S.C. 102 (b) over Adams.

At the very beginning of the specification clearly appears the object of the claimed invention, which is to propose a method for the pseudo-random computation of a permutation of a word comprising N digits (base 10) and not at all of bits (base 2). The field of the invention is that of cryptography. More particularly, the field of the claimed invention is that of cryptography applied to the encryption of words formed by digits.

The different goals are summed up below, each only regarding digit words and never bit words:

- to enable the robust encryption of a word formed by N digits,
- to provide a fast encryption of a word formed by N digits,
- to determine a robust pseudo-random permutation in a set whose cardinal is $10N$, this cardinal therefore not being a power of 2 (as a power of 2 is the only disclosure in Adams),
- to perform the enciphering of identifiers based on the use of digits, such as, for example, telephone numbers, credit cards...,
- to generate a string of N digits that is a pseudo-random string,

-to produce N-digit strings such that the production process ensures that the same string will not be produced twice.

Then, from page 2, line 3, to page 4, line 13, the disclosure points out the differences between bits and digits and also recites the different techniques available, which present huge drawbacks when trying to implement them in applications like the ones concerned in the claimed invention. In this way, it is also explained that in certain industrial-scale applications, for example in telephony, it is sought to have not a certain number of bits but a certain number of digits at the input and the output. All the standard cryptographic functions in secret key cryptography take a certain number of bits at the input and give a certain number of bits at the output. This was and is always the case, for example, of the SHA-1 function, the DES function, the AES function, etc.

For a better understanding of the actual differences between the prior art and the claimed invention, the following explanation is given. The known prior art only allows or simply only knew how to work on binary spaces (bits) and, in particular, binary blocks of 64K bits length. As an example, it is easy to build cryptographic functions, like DES, from a first space $[0 \dots 2^{64}-1]$, a symmetric cryptographic function being indeed a bijection between both spaces.

However, one cannot easily build a correspondence between a digits space (expressed by a power of 10) and binary (bits) space (expressed by a power of 2). Should one implement a reversible cryptographic function, one must use a bijection, that is to say one absolutely needs to work using starting and ending spaces having the same size. Because of the restricted use of the entropy in a binary world (binary encryption of a decimal number) when working on digits, one cannot build a bijection since elements of the starting binary space will never correspond to an element of the ending space expressed in digits. This is obviously because the size of the starting set in the bijection is always lower than the size of the ending set.

This can be illustrated by the following four-bits example:

-starting space: 16 possible values (from 0000 to 1111[`binary`]), thus 16 elements in the starting set,

-ending space: 16 possible values (from 0000 to 1111 [`binary`]), thus 16 elements in the ending set.

A symmetrical encryption will thus correspond to a bijection between these 2 spaces. If the starting space is restricted to a sub-set such as digits (bits 0000 to 1001), then it is quite impossible to build a bijection between a set having a "size 10" and a set having a "size 16". A digit encrypted on a byte the value of which is included between 0 and 9 or according to an ASCII encryption "0" and "9" would have a value between 0 and 255 after being binary encrypted.

If a function capable of converting digits from any one length to bits of a length of a power of 2 did exist, then one could not find unobviousness since it would be enough to build a conversion function, to encrypt and then to build the inverse function. It is unfortunately not at all possible to build such conversion functions of this kind capable of being inversed as the entropy is by definition (as explained above) different. As an example, numbers comprised between [00000 to 99999] will never be convertible into numbers of a power of 2.

Also, an industrial cryptographic solution does not exist (in bits, as the one disclosed in Adams) capable of encrypting, for instance, a 15 digits international telephone number or a credit card number by using a powerful algorithm such as DES or 3DES. The result would not be in accordance with the initial syntax with the right context length to be encrypted.

To solve this problem, one solution would be to rewrite specific functions, but designing and developing these functions could take up a lot of time. They would necessarily be

far less analyzed by the international cryptographic community, and thus could not be provided in a sufficiently efficient and secure way. But in the context of the claimed invention efficiency and security are typically features which are needed.

Or else, according to the claimed invention, it is possible to have inputs and outputs of digits, but ones that use classic cryptographic functions on the bits to ensure security. It is such an unobvious method, for a particular problem, which no one had ever thought of and with no solution up to the present date, that is efficiently proposed and implemented in the claimed invention. It solves this particular problem, which has been around for a long time but until now there was no efficient solution.

This is actually the case with the claimed invention where the round functions of the generalized Feistel scheme here used take a digits at the input and give b digits at the output, which is not at all obvious and, of course, not at all disclosed in Adams.

For this very purpose, and to give an efficient example to better understand the actual content of the novel and unobvious features the claimed invention proposes (as explained at page 10, with the description of step 202), the function F_i is expressed (for example) as follows:

$$F_i(x) = \text{SHA}_1(i \parallel K \parallel x \parallel j) \oplus (1)$$

In this expression:

"SHA_1()" : is the hash function of the same name. In practice, another hash algorithm such as MD5, for example, may be used. It is also possible to use another function such as AES (Advanced Encryption Standard) or TDES (Triple Data Encryption Standard). These are standard pseudo-random functions of cryptography on binary words. More generally, it is possible to use any function or a pseudo-random function on bits.

"||": is a concatenation operator.

"K": is the key that is read in the memory 106.

"i": is the index of the round of the Feistel function.

The notation $\langle || j \rangle$ signifies that j is initialized at 0, and then that the 17 most significant bits are extracted from the output of the function SHA_1. If these 17 bits correspond precisely to five digits (the desired property), this output is kept. If not, j is increased by one unit and the expression (1) is re-evaluated until this property is obtained.

The iteration on j actually corresponds to a conversion of a binary number into a digit number.

The input words of the round functions are therefore produced by the conversion of the digit words into binary words. The output binary words of the round functions are therefore converted into digit words. In order that 17 bits may correspond precisely to five digits, the conversion of this 17-bit word into decimal notation must be expressed with five figures.

In the claimed invention the only place in which the binary to digit and digit to binary conversions are realized is confined inside each F_i function. This means that all other operations needed by the Feistel scheme are realized in digit spaces.

The object of the invention therefore is a method for the generation of a pseudo-random permutations of an N -digit word in which:

- a generalized Feistel scheme (202-205) is implemented,

wherein:

- the round functions of the generalized Feistel scheme implemented are functions (F_i) such that:

- the input words of the round functions are produced by the conversion of digit words into binary words,
- then a one-way function is applied to these binary words (as explained just above),
- finally, the output in digits is a function of these binary words,
- a digit word to be enciphered is read in a memory (104),
- the generalized Feistel scheme used comprises at least $T=5$ rounds.

In addition, it is important to note that claimed invention was not obvious at all since the simple checking of its fully correct working took several weeks. This was done by a well-distinguished specialist in this particular field who fully isolated himself from the rest of the world. This was done after having implemented this invention to demonstrate that it was correctly working. This efficient solution has been implemented (and is actually fully operational) for more than 3 years.

Within the specification, one can find a great deal of applications and uses which show the immediate advantages brought about when implementing the claimed invention compared to the well-known techniques of Adams or any other prior art.

This claimed enciphering method is used to encipher commonly used digit words. Such words are (national) telephone numbers (8 to 10 digits), credit card numbers (16 digits), social security numbers (13 digits, for example in France), bank account numbers, electronic vouchers, etc. The list is not at all exhaustive. Furthermore, these numbers may be concatenated into a greater number so as to obtain a 30-digit word.

In general, with the method according to the claimed invention, the longer the word to be enciphered, i.e., the greater the length of N , the greater the resistance to cryptographic analysis.

For an input word, a given enciphering key and a number of rounds of the Feistel scheme, it is always the same enciphered word that is obtained. So as to reinforce the

enciphering and, above all, to prevent behavioral research based on an electronic identifier, a digit number to be enciphered can be concatenated with a random digit number. For example, to encipher a telephone number, it is first concatenated with the number of seconds that have elapsed since the beginning of the current hour. Then the result of this concatenation is enciphered. Thus, the same enciphered word is only obtained very rarely, for instance, for a given telephone number. The type of random number used is any random number. It may be obtained, for example, by means of a simple counter of a number drawn from a pre-computed pseudo-random sequence, the counter increasing with each instance of use.

Among the possible uses of the method according to the claimed invention, there is the possibility of enciphering information between the sender of information and its addressee. There is also the possibility of isolating two networks from each other. This isolation is achieved, for example, by use of a server in a first network. In the method according to the claimed invention, this server transcodes an identifier of the first network to produce an identifier of the second network. Thus, the entities acting on the second network, except for the operator of the first network, are incapable of identifying the user of the first network.

The claimed invention can therefore be applied very particularly and very advantageously to telephony. Thus, in the context of protecting the privacy of subscribers with a telephony operator and combating "spam", all the protocols use the MSISDN (the subscriber's international telephone number) encoded on 15 digits as a subscriber identifier. Then this identifier could be misused by the service provider in order to set up a user profile to send "spam" type messages. It may be sought to conceal this value by enciphering, but the result must then be compatible with the format of the telecommunications protocols. In particular, the operator should be capable of easily deciphering this value. These two aims are achieved with the method according to the claimed invention.

The case of the electronic voucher is also a good exemplary application of the claimed invention. The interface at the level of a mobile telephone is limited to the numerical keypad. The user is therefore limited in his keying-in operation to digits. In the generation of an electronic voucher (a voucher number is equivalent to a financial value, for example 30 dollars), each keying in of a voucher is used to credit a sum to an account. The management of the vouchers with the service provider is simplified if the generator of these values uses symmetrical algorithms working on digits. A counter runs from 1 to M, and the enciphering of the counter gives pseudo-random data that are all different. It is thus possible to generate pseudo-random codes on N digits, easily manageable by the service provider because it is only the last counter value used this is stored and not all the values of vouchers already generated to ensure the uniqueness of these vouchers.

In general, in "large" databases, the storage is done in unencrypted form. The structure may be composed (with digital and alphanumeric non-homogenous formats), and the safety requirements dictate enciphering of the data. This is achieved without any modifications of the structure and for very low cost.

As explained above, the claimed invention provides a generalized Feistel scheme which works and always stays in digit spaces all over the rounds and process of ciphering, and this is what allows the claimed invention to gain all the above advantages. What is here fundamental is the fact that in the claimed invention, the algorithm stays in a digit space from a mathematical point of view. The claimed invention only accesses the binary space during the round function computation, which function takes at the input digits and produces output results in digits. The fact that the processor works in binary and then has a binary representation of digit is not part of the claimed invention (and simply has nothing to do with it) since the claimed invention wants to stay at a formal mathematical level to gain all the above described advantages.

Contrary to what the claimed invention teaches and which is the only purpose of the claimed invention, Adams discloses a method which works on binary and only on binary words (see the abstract "...input message block of binary data of predetermined length $2n$ ". This is true for all of the Adams disclosure, see particularly columns 1, 2, 3 and 4). To sum up, Adams discloses and teaches, but only teaches, a method of transforming an input message block of binary data of predetermined length $2n$ bits into an output message block of binary data.

In addition, in Adams, for instance, column 6, lines 11-41, it immediately appears that the process disclosed and taught within this patent which only works with binary data differs from the presently claimed process. Specifically, claim 1 recites "...the input words of the round functions are produced by a conversion of digit words into binary words...the output in digits is a function of these binary words, a digit word to be enciphered is read in a memory..." , which limitations are not in Adams.

Thus the rejection of claims 1 and 2 under 35 U.S.C. 102 over Adams should be withdrawn.

Claim 5 is not unpatentable under 35 U.S.C. 103(a) over Adams.

Since Adams fails to suggest the above-discussed digit words feature, claim 5 is also patentable (see MPEP 2143.01).

Claims 6-7 are not unpatentable under 35 U.S.C. 103(a) over Adams in view of Coppersmith.

Coppersmith is also related to binary and only to binary words. Nowhere does Coppersmith teach or even suggest the way to efficiently deal with digits words using the specific technical features proposed in the claimed invention.

Thus even if Coppersmith is combined with Adams, the result is not the claimed invention. Hence the rejection of claims 6 and 7 should be withdrawn.

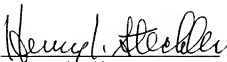
Regarding claim 8-10, as the Examiner admits, Adams does not disclose the claimed lengths. Neither does Coppersmith. Thus combining the references does not result in the claimed invention.

Hence the rejection of claims 8-10 should be withdrawn.

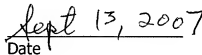
For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for the one month extension fee (\$120) as well as any other fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,



Henry I. Steckler
Reg. No. 24,139


Date

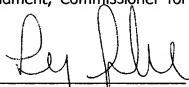
Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being transmitted electronically, on the date indicated below, addressed to the Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 13 Sept 2007

Signature: _____


Liso Shimizu
Person Making Deposit